ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41257—2022

数字化车间功能安全要求

Functional safety requirements for digital factory

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：机械工业仪器仪表综合技术经济研究所、中国石油集团安全环保技术研究院有限公司、浙江中控技术股份有限公司、北京和利时系统工程有限公司、国能智深控制技术有限公司、深圳市标利科技开发有限公司、中国科学院沈阳自动化研究所、上海工业自动化仪表研究院有限公司、上海自动化仪表有限公司、中石化广州工程有限公司、长沙有色冶金设计研究院有限公司、北京市劳动保护科学研究所。

本文件主要起草人：孟邹清、史学玲、郭苗、魏振强、裘坤、王志平、熊文泽、朱杰、刘盈、田雨聪、文科武、徐皑冬、周有铮、杨明、王敏良、马百旺、闫炳均、靳江红、李佳、彭小波、马欣欣、冯健、陈汝、牛海明、鄢锋、杨静雅、谢亚莲、陆妹、张亚彬、张雪、姜瑞景。

引　言

数字化车间是智能制造的核心单元，涉及领域广泛，类型复杂多样。智能化技术在给制造业带来难得发展机遇的同时，也使制造业面临着安全方面的挑战。数字化车间中存在多种风险，面临多种安全问题，如：数字化制造设备的运行失效（包括控制功能失效、安全功能失效），可能会导致制造系统的功能失控、产品质量下降等，从而对周围的人员、资产或环境造成危害，带来巨大的经济损失，造成声誉方面的影响。

《中国制造 2025》纲要明确提出要建立智能制造安全保障系统。为了降低数字化车间中的风险，保障数字化车间的安全运行，需采用功能安全的技术手段，通过危险与风险分析、保护层评估，明确数字化车间的功能安全要求，在数字化车间中设置保护层（如：安全相关系统、物理保护系统等），建立功能安全管理系统，全方位多角度保障数字化车间的功能安全。

依据 GB/T 37393—2019《数字化车间　通用技术要求》，数字化车间重点涵盖产品生产制造过程，其体系结构分为基础层和执行层。因此，本文件中数字化车间的功能安全要求也将限定在基础层和执行层的范围内。

数字化车间的功能安全，主要考虑以下三个方面。

一是针对数字化车间中已识别的危险及风险分析结果，结合行业或企业自身的可容忍风险，进行保护层评估，确定各类保护措施的必要性以及所需的安全保护功能。在数字化车间的基础层中设置适当保护层（如：安全相关系统、物理保护系统等），用以降低数字化车间生产过程中可能带来的对资产、人员、环境产生的风险。尤其针对数字化车间自身特点，重点关注车间的制造设备或装置在互相联通后带来的新的风险，以及由于数字化、网络化、智能化的升级促成实现的安全保护新模式。

二是在数字化车间的执行层中建立一个功能安全管理信息系统，对数字化车间的安全风险、保护层、安全相关系统以及其他功能安全相关活动进行数据采集分析、可视化管理、动态管控。

三是构建一个功能安全信息物理系统，通过 E/E/PE 安全相关系统、其他风险减低措施和功能安全管理信息系统等的有机融合与深度协作，实现数字化车间功能安全的实时感知、动态控制和信息服务。

功能安全信息物理系统，包括：

——基础层的 E/E/PE 安全相关系统（包含安全检测、控制和执行）、其他风险减低措施及其检测单元、安全服务器、安全接口和通信；

——执行层的功能安全管理信息系统及其安全数据、服务等。

数字化车间功能安全的示意图，如图 1 所示。

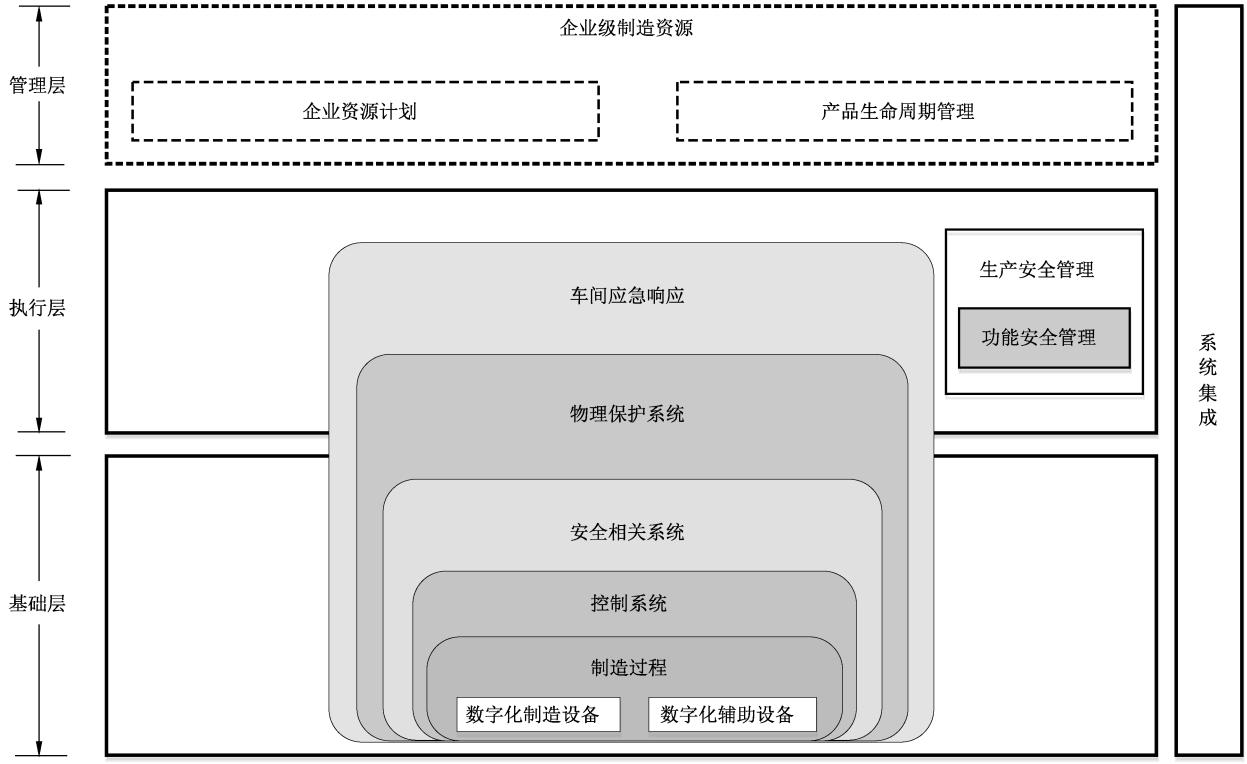

图 1　数字化车间功能安全示意图

数字化车间功能安全相关活动的过程和结果，通过采用计算机可识别的形式采集、存储、调用、处理和展示，以实现完整记录、保存以及可追溯，适应数字化车间建设需要。

数字化车间功能安全要求

1 范围

本文件规定了安全生命周期、数字化车间的功能安全管理、数字化车间危险与风险分析、数字化车间保护层评估、安全相关系统要求、功能安全管理信息系统要求、功能安全集成要求等内容。

本文件适用于指导数字化车间的新建和改扩建。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20438.1 电气/电子/可编程电子安全相关系统的功能安全 第1部分：一般要求

GB/T 20438.2 电气/电子/可编程电子安全相关系统的功能安全 第2部分：电气/电子/可编程电子安全相关系统的要求

GB/T 20438.3 电气/电子/可编程电子安全相关系统的功能安全 第3部分：软件要求

GB/T 20438.4 电气/电子/可编程电子安全相关系统的功能安全 第4部分：定义和缩略语

GB/T 37393—2019 数字化车间 通用技术要求

GB/T 37413—2019 数字化车间 术语和定义

3 术语、定义和缩略语

3.1 术语和定义

GB/T 20438.4 界定的以及下列术语和定义适用于本文件。

3.1.1

数字化车间 digital factory；digital workshop

以生产对象所要求的工艺和设备为基础，以信息技术、自动化、测控技术等为手段，用数据连接车间不同单元，对生产运行过程进行规划、管理、诊断和优化的实施单元。

注：在本文件中，数字化车间仅包括生产规划、生产工艺、生产执行阶段，不包括产品设计、服务和支持等阶段。

[来源：GB/T 37413—2019，2.1]

3.1.2

控制系统 control system

响应来自过程和(或)操作者的输入信号，并产生输出信号，使制造过程按预期方式工作的系统。

[来源：GB/T 20438.4—2017，3.3.3，有修改]

3.1.3

制造执行系统 manufacturing execution system

生产活动管理系统，该系统能启动、指导、响应并向生产管理人员报告在线、实时生产活动的情况。这个系统辅助执行制造订单的活动。

[来源：GB/T 25486—2010，2.162]

3.1.4

保护层　layer of protect

用来防止不期望事件的发生或降低不期望事件后果严重性从而降低过程风险的设备、设施或方案。

[来源:GB/T 32857—2016,3.1.3]

3.1.5

功能安全管理信息系统　functional safety management information system

对数字化车间的安全风险、保护层、安全相关系统以及其他功能安全相关活动进行数据采集分析、可视化管理、动态管控的信息系统。

3.1.6

功能安全信息物理系统　functional safety cyber physical systems

是一个综合计算、网络和物理环境的多维复杂系统,通过 E/E/PE 安全相关系统、其他风险减低措施和功能安全管理信息系统等的有机融合与深度协作,实现数字化车间功能安全的实时感知、动态管控和信息服务。

3.2　缩略语

下列缩略语适用于本文件。

DC	诊断覆盖率	Diagnostic Coverage
E/E/PE	电气/电子/可编程电子	Electrical/Electronic/Programmable Electronic
MRT	平均维修时间	Mean Repair Time
$MTTF_D$	平均危险失效间隔时间	Mean Time To Dangerous Failure
PL	性能等级	Performance Level
SIL	安全完整性等级	Safety Integrity Level
SRP/CS	控制系统安全相关部件	Safety-Related Part of a Control System

4　安全生命周期

应依据 GB/T 20438.1 规定,统筹考虑数字化车间功能安全的相关活动,定义数字化车间及其功能安全信息物理系统的生命周期阶段以及各阶段相关内容和要求。

注:典型的安全生命周期阶段包括。

——危险与风险评估。确定生产制造过程及设备、控制层、执行层的危险和危险事件、导致危险事件后果、与危险事件相关的过程风险、风险降低和要达到必要的风险降低所需要的安全功能要求。

——给保护层分配安全功能。给保护层分配安全功能并为每个电气/电子/可编程电子安全功能分配相关的安全完整性等级。

——安全需求。为了达到要求的安全功能,根据要求的电气/电子/可编程电子安全功能及其相关的安全完整性规定每个安全相关系统的要求。

——设计和工程。设计安全相关系统,以满足安全功能和安全完整性要求。

——安装、调试和确认。集成和测试系统;根据要求的安全功能和要求的安全完整性,确认安全相关系统在各方面都满足功能安全要求。

——操作和维护。保证在操作和维护期间保持安全相关系统的功能安全。

——变更和停用。对安全相关系统进行校正、增强或自适应以保证达到和保持要求的安全完整性等级。

——验证。测试和评估给定阶段的输出,确保其对于该阶段关于产品和标准输入的正确性和一致性。

——功能安全评估。对安全相关系统所达到的功能安全进行调查并作出判断。

5 数字化车间的功能安全管理

5.1 组织人员和资源

5.1.1 规定实现数字化车间功能安全的方针和策略，包括评估它们实现的方法和在组织内交流的方法。

5.1.2 识别出实施数字化车间功能安全活动的所有人员、部门和组织的责任（如哪些活动应由相关的许可授权或法定的安全机构负责完成），和执行各阶段活动人员的适当的能力（即培训、技术知识、经验和资质）。

5.2 执行和监督

5.2.1 应制定规程，以保证对数字化车间的风险降低措施的相关建议能迅速跟进和满意解决，建议包括来自：

——危险和风险分析；

——功能安全评估；

——验证活动；

——确认活动；

——风险降低措施的配置管理；

——事故报告和分析。

5.2.2 应制定规程，以保持对危险和危险事件、风险降低措施和数字化车间信息的准确性。

5.2.3 在特定的场合中，应提供应急服务的培训和信息。

5.2.4 负责对数字化车间提供产品或服务的供应商，应提供该组织规定的产品和服务，并有适当的质量管理系统。

5.3 数字化车间的功能安全管理

数字化车间的 E/E/PE 安全相关系统、其他风险减低设施在其全生命周期阶段内，都宜进行数字化管理；安全相关活动宜进行数字化处理；以上信息宜纳入功能安全管理信息系统。

6 数字化车间危险与风险分析

6.1 生产制造过程及设备

6.1.1 分析内容

应对数字化车间生产制造过程及相关设备开展危险与风险分析，分析内容应包括但不限于：

——数字化车间工艺单元的危险识别与风险评估，安全功能识别，以及识别条件等；

——数字化车间单体设备（如机器人、切削机床、压缩机、容器等）的危险识别与风险评估，安全功能识别，以及识别条件等；

——数字化车间工艺单元之间、单体设备之间、工艺单元与单体设备之间或者单体设备与人之间由于彼此关联或影响，可能引发的危险的识别与风险评估，安全功能识别，以及识别条件等。

6.1.2 分析结果

分析结果应包括但不限于：

——已识别的每个危险事件及其起因（包括人为错误）的描述；

——事件的后果和可能性描述；
——工况考虑；
——风险降低要求的确定；
——为降低风险所采取措施的描述或者引用；
——在风险分析中对保护措施的可能的要求率和设备失效率等所作的假设，以及对操作约束或人为干预的可信度的详细描述。

6.2 控制层和执行层

6.2.1 分析内容

应对数字化车间的控制层和执行层开展危险识别与风险评估，评估内容应包括但不限于：
——控制系统、制造执行系统的自身失效或错误行为；
注 1：包括控制系统各子系统或功能单元的失效或错误、子系统或功能单元之间不期望关联或作用、系统性失效或错误等。
——控制系统、制造执行系统的自身失效或错误行为可能带来的危险事件及其后果；
注 2：有些情况下，需要对危险事件的发生条件、发展过程、事件后果、及发生可能性等内容进行细化分析。
——控制系统、制造执行系统的自身失效或错误行为的避免或控制措施分析；
注 3：必要时进一步开展措施有效性分析，需要的外部保护功能分析等。
——确定由安全相关系统实现的外部保护功能（若有）；
——控制系统、制造执行系统遭受外部信息安全攻击、合理可预见的误用或未经授权的行为等引起的失效或错误行为分析，以及可能带来的危险事件及后果；
注 4：必要时，进一步开展危险事件的发生条件、发展过程、事件后果及可能性分析。
——针对控制系统、制造执行系统遭受外部信息安全攻击、合理可预见的误用或未经授权的行为等引起的失效或错误，需要的风险防范措施分析等；
——应在仿真、调试、运行、维护等生命周期各个环节考虑可能带来的危险与风险。

6.2.2 分析结果

分析结果应包括但不限于：
——控制系统、制造执行系统的子系统或功能单元失效或错误行为描述，以及引发该失效或错误行为的原因描述；
——控制系统、制造执行系统的自身失效或错误行为可能带来的危险事件及其描述；
——控制系统、制造执行系统的自身失效或错误行为的避免或控制措施描述；
——有关发生可能性的信息描述或引用；
——由安全相关系统实现的保护功能描述；
——分析评估过程中所作的假设描述；
——系统状态、操作约束、人的行为等条件约束；
——控制系统、制造执行系统的遭受外部信息安全攻击、合理可预见的误用或未经授权的行为可能带来的危险事件及其描述；
——控制系统、制造执行系统的遭受外部信息安全攻击、合理可预见的误用或未经授权的行为的避免或控制措施描述。
注 1：数字化车间危险与风险分析的方法和步骤，见附录 A。
注 2：对于遭受外部信息安全攻击、合理可预见的误用或未经授权的行为影响和防范的完整的分析需要开展信息安全风险评估，参见 GB/T 41260—2022 等相关标准。

7 数字化车间保护层评估

7.1 数字化车间保护层

根据危险与风险分析的结果，提出数字化车间所需的保护层。

注：数字化车间保护层的类型包括但不限于：安全相关系统、物理保护系统、车间应急响应等。

7.2 制造过程和设备的保护层评估

7.2.1 评估内容

应对数字化车间制造过程和设备各危险事件的保护层的设计开展评估，评估内容应包括但不限于：

——基于 E/E/PE 技术的保护层功能，以及需要其提供的风险降低目标；

——基于其他技术（如：液压、气动等）的保护层功能，以及需要其提供的风险降低目标；

——其他风险降低措施的保护层功能，以及需要其提供的风险降低目标；

——若存在多层保护，则各保护层之间的共用部分识别，并评估其所带来的风险降低损失；

——若存在多层保护，则各保护层之间可能的共同原因或共同模式的失效，并评估其所带来的风险降低损失；

——基于 E/E/PE 技术的保护层运行模式，以及对应的目标失效量，相应的 SIL 要求。

7.2.2 评估结果

评估结果应包括但不限于：

——基于 E/E/PE 技术的保护层安全功能描述；

——保护层运行模式；

——保护层目标失效量；

——保护层独立性描述，以及为保持独立性所需的条件或约束的描述；

——为确定保护层的风险降低目标所做的假设，以及其置信度描述。

7.3 控制层和执行层的保护层评估

7.3.1 评估内容

7.3.1.1 对控制层和执行层的自身失效或错误引发的、由安全相关系统实现的保护层的设计，应开展评估，评估内容应包括但不限于：

——基于 E/E/PE 技术的保护层功能，以及需要其提供的风险降低目标；

——若存在多层保护，则各保护层之间的共用部分识别，并评估其所带来的风险降低损失；

——若存在多层保护，则各保护层之间可能的共同原因或共同模式失效，并评估其所带来的风险降低损失；

——对于基于 E/E/PE 技术的保护层的运行模式，以及对应的目标失效量，相应的 SIL 要求。

7.3.1.2 对控制层和执行层遭受外部物理环境（如：温湿度、腐蚀、粉尘、电磁脉冲、射线）影响的保护层的设计，应开展评估，评估内容应包括但不限于：

——保护层功能，以及需要其提供的风险降低目标；

——若存在多层保护，则各保护层之间的共用部分识别，并评估其所带来的风险降低损失；

——若存在多层保护，则各保护层之间可能的共同原因或共同模式失效，并评估其所带来的风险降低损失；

——对于基于 E/E/PE 技术的保护层的运行模式，以及对应的目标失效量，相应的 SIL 要求。

7.3.1.3 对控制层和执行层遭受外部信息安全攻击、合理可预见的误用或未经授权的行为影响的保护层的设计，应开展评估，以确定保护层功能及需要的保护等级。具体参考工控信息安全相关标准规范。

7.3.2 评估结果

评估结果应包括但不限于：

——基于 E/E/PE 技术的保护层安全功能描述；
——保护层运行模式；
——保护层目标失效量；
——保护层独立性描述，以及为保持独立性所需的条件或约束的描述；
——为确定保护层的风险降低目标所做的假设，以及其置信度描述。

8 安全相关系统要求

8.1 安全功能要求

应对分配给安全相关系统的安全功能进行详细的定义，包括：

——各安全功能的描述；
——各安全功能的操作频率；
——各安全功能要求的响应时间；
——安全功能应启动或禁用的工况（例如运行模式）；
——可能同时启动，造成冲突行为的功能之间的优先权问题；
——安全功能对其他过程功能或控制功能的接口；
——对故障反应功能以及操作的各种限制（如机器重新启动或者继续运转）等的描述，以防初始错误即导致机器停止运行；
——操作环境描述（例如温度、湿度、灰尘、化学物质、机械振动和震动）；
——测试以及各种相关设施（例如测试设备、测试接入端口）；
——相关机电设备的操作循环周期、工作循环周期及/或应用类型；
——断电、急停、失控、非受控工况的功能描述。

8.2 安全完整性要求

8.2.1 一般要求

应对安全相关系统的安全功能明确风险降低目标。对 E/E/PE 安全相关系统的安全功能，还应明确其安全完整性等级。

8.2.2 安全完整性等级

8.2.2.1 每个 E/E/PE 安全相关系统的安全功能的安全完整性等级要求应来自风险评估和保护层评估，以确保完成必要的风险降低。

注 1：安全完整性等级要求离散的分为四级，SIL4 为最高安全完整性等级，SIL1 为最低安全完整性等级。

注 2：安全完整性等级要求的目标失效量，按照运行模式的不同，分为要求时的失效概率和每小时的危险失效率。

注 3：不同的行业有不同的安全完整性等级要求。

8.2.2.2 低要求运行模式下，分配给 E/E/PE 安全相关系统的每个安全功能的安全完整性要求应按照安全功能的要求时危险失效平均概率（PFD_{avg}）作为目标失效量见表 1，提出风险降低要求。

表 1　安全完整性等级:在低要求运行模式下安全功能的目标失效量

安全完整性等级(SIL)	安全功能在要求时的危险失效平均概率(PFD_{avg})
4	$\geqslant 10^{-5} \sim < 10^{-4}$
3	$\geqslant 10^{-4} \sim < 10^{-3}$
2	$\geqslant 10^{-3} \sim < 10^{-2}$
1	$\geqslant 10^{-2} \sim < 10^{-1}$

8.2.2.3　高要求或连续运行模式下,分配给 E/E/PE 安全相关系统的每个安全功能的安全完整性要求应按照安全功能的每小时危险失效平均频率(PFH)作为目标失效量见表 2,提出风险降低要求。

表 2　安全完整性等级:在高要求或连续运行模式下安全功能的目标失效量

安全完整性等级(SIL)	安全功能的每小时危险失效平均频率(PFH)
4	$\geqslant 10^{-9} \sim < 10^{-8}$
3	$\geqslant 10^{-8} \sim < 10^{-7}$
2	$\geqslant 10^{-7} \sim < 10^{-6}$
1	$\geqslant 10^{-6} \sim < 10^{-5}$

注:在有些行业领域,安全完整性等级的表示会有不同,如在机械安全领域,采用“PL”来衡量安全级别要求。SIL 与 PL 的区别与联系见附录 B。

8.2.3　安全完整性考虑的几个方面

数字化车间安全相关系统的选择或设计(包括:整体硬件、软件体系结构、传感器、执行元件、可编程电子器件、嵌入式软件、应用软件等),均应符合以下要求:

a)　硬件安全完整性要求,包括:
　——硬件安全完整性体系结构限制;
　——危险随机硬件故障概率要求。
b)　系统安全完整性要求,包括:
　——故障避免要求;
　——失效控制要求。

注:软件安全完整性作为系统性安全完整性的一部分考虑。

8.3　独立性要求

8.3.1　独立内容

安全相关系统应与非安全相关系统独立设置。独立的内容包括:

——控制单元独立;
——现场检测单元独立;
——现场执行单元独立;
——联接和配线独立。

8.3.2　最高安全完整性等级原则

8.3.2.1　当安全相关系统同时执行非安全功能时,非安全部分应按照安全部分的完整性要求来设计实

施，或采取措施来保证非安全功能的任何行为不会影响到安全功能的完整性。

8.3.2.2 当安全相关系统实现不同安全完整性等级的安全功能时，除非能表明较低安全完整性等级的安全功能对较高安全完整性等级的安全功能没有负面影响，否则共享或共用硬件和软件应符合最高安全完整性等级。

8.4 故障响应要求

8.4.1 在能容许单一硬件故障的任何子系统中，检测到危险故障时（利用诊断测试、检验测试或任何其他办法）应导致执行一个规定动作，以达到或保持安全状态；或隔离故障部分以使得在修复故障部分的同时继续过程机器的安全运行。如果故障部分的修复不能在计算硬件随机失效概率中设定的 MRT 内完成，则会产生一个规定的动作以达到或保持某个安全状态。

8.4.2 在子系统没有容错能力的场合，当在子系统中检测到危险故障时（利用诊断测试、检验测试或任何其他办法），则应导致一个规定动作，以达到或保持某种安全状态。如：导致机器的运行停止，且机器的正常操作（如重新启动机器）将不能进行，直到该故障已经修复或校正。

8.5 其他要求

8.5.1 控制层应满足 GB/T 20438.1、GB/T 20438.2、GB/T 20438.3 中关于 E/E/PE 安全相关系统及其子系统的设计和集成的相关要求。

8.5.2 应采取措施，实现对包括检测、控制、执行设备的安全相关信息的采集。

9 功能安全管理信息系统要求

9.1 一般要求

9.1.1 应在数字化车间的执行层中建立一个功能安全管理信息系统，作为数字化车间生产安全管理的构成部分。

注：功能安全管理信息系统将功能安全管理流程从以人工干预为核心转变为以自动化、信息化处理为核心，并与执行层其他功能模块进行必要信息交互，自动化执行或主动指导功能安全相关业务，提高企业安全等级。

9.1.2 功能安全管理信息系统应基于企业业务流程和功能安全管理规范，针对企业资产、人员、环境等的安全需求构建。

9.2 功能要求

9.2.1 基本要求

9.2.1.1 功能安全管理信息系统应能实时采集功能安全状态数据，提供功能安全监测和风险预警，提高功能安全管理可视化水平。

注：例如采集检测、控制、执行设备的安全相关信息。

9.2.1.2 功能安全管理信息系统的功能包括但不限于：危险与风险管理功能、保护层管理功能、安全相关系统管理功能。

注：根据行业或企业特点或实际需求，增加以下功能：功能安全培训、人员上岗/作业管理、应急响应、功能安全复审管理等。

9.2.2 危险与风险管理功能

对于不同的过程风险进行实时有效监控，并与预设的标准值进行比对，实现超限报警、反馈调节等功能。

9.2.3 保护层管理功能

对数字化车间各类关键保护层进行实时状态监视，并与中高风险的危险场景进行关联，建立过程风险等级与保护层降险等级之间的比对关系，监视关键过程残余风险的实时动态变化情况。

9.2.4 安全相关系统管理功能

9.2.4.1 安全完整性状态监测子功能

对于分配有明确的安全完整性等级(SIL)的安全功能，应符合功能安全相关标准的规定，并由安全完整性等级(SIL)指标来衡量。安全完整性状态监测子功能针对执行安全功能的控制系统(包括智能检测仪表和执行机构)，应：

——关注并采集系统功能设置、运行模式、响应时间、设备状态、诊断及反馈、故障频率及响应等信息；

——提供在实际运行条件下安全完整性的可视化，监视随时间变化的安全完整性状态；

——与危险与风险管理单元信息交互，及时观察风险环境变化，评估风险状况，随时更新实际运行条件下的风险等级，实现风险可视化管理；

——对于安全完整性降低的部件，发出预警或报警，并与设备维护管理单元信息交互，提出对部件的维修维护请求。

9.2.4.2 检测和维护子功能

跟踪并指导安全相关系统、备品备件及其检测维护工具的维护活动，确保其可用性；实现安全相关系统不同安全等级条件下的周期性维护、状态维护或故障检修维护的提醒(报警)及调度功能；建立维护事件或问题的历史信息库，以支持故障诊断。

9.2.4.3 变更管理子功能

跟踪并指导安全相关系统的变更活动；建立变更活动历史信息库，支持变更追溯；实现变更状态提醒，其他功能模块相关信息应随变更同步更新，可视需要采用实时同步或定期同步的方式。

9.3 数据要求

应对数字化车间功能安全相关的数据要素进行采集，并以计算机可识别的形式存储、调用、处理和展示，以适应数字化车间建设需要。

注：数字化车间功能安全相关的数据要素包括但不限于。

——危险信息。危险类别、危险区域、危险原因、危险事件、可能的伤害等。

——风险信息。风险等级、风险后果等级、发生可能性或可能性等级等。

——保护层信息。保护层名称、编号、功能描述、其他相关保护等。

——安全功能信息。功能编号、功能描述、工作状态等。

——安全完整性信息。目标失效量、安全完整性等级、检验测试周期等。

——安全系统构成。传感器、控制器、执行机构等构成系统的设备；各设备的数量、结构方式(冗余、热备、表决等)、逻辑关系。

——安全仪表设备信息。设备名称、编号、厂家、生产日期、性能参数等。

——安全相关设备失效信息。平均失效率、故障记录等。

——维检修信息。维检修周期、维检修内容、维检修规程、维检修时间等。

——管理信息。人员管理、维检修作业管理等。

——人员信息。姓名、工作编号、岗位、资质等。

——知识类信息。过程设备失效数据库等。
——关系信息。

10 功能安全集成要求

10.1 一般要求

10.1.1 应通过功能安全集成，形成功能安全信息物理系统。
10.1.2 数字化车间的功能安全集成如图 2 所示，包括以下几方面：
——人与安全相关系统互联时的人机接口；
——安全相关系统与非安全相关系统互联时的现场设备通信接口；
——功能安全管理信息系统与安全相关系统互联时的网络通信接口。

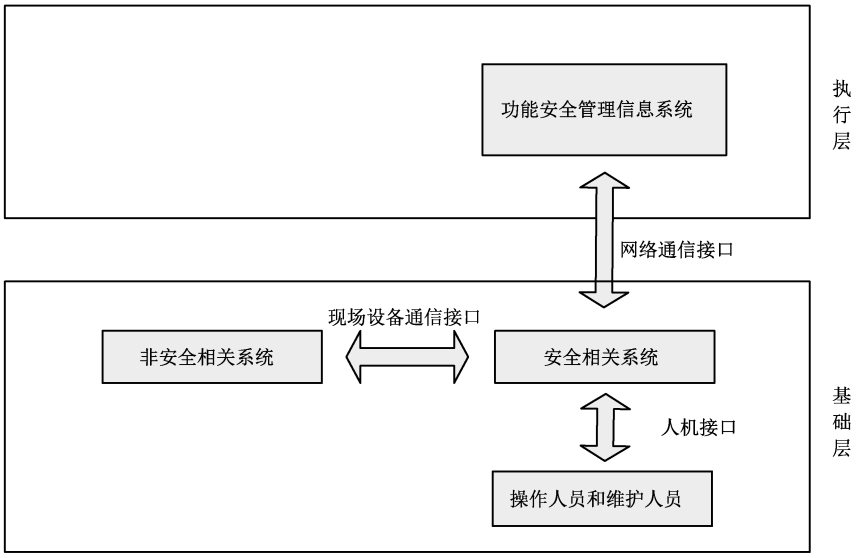

图 2 数字化车间功能安全集成示意图

10.2 人机接口要求

10.2.1 人员因素

10.2.1.1 在考虑人员因素时，人机接口宜考虑以下几个方面：
——可操作性；
——可维护性；
——可测试性。
10.2.1.2 人机接口设计应遵循良好的人员操作惯例，并适合人员可接受的培训或认知水平。

10.2.2 操作和访问限制

10.2.2.1 应单独设置操作接口和维护接口。
10.2.2.2 接口应具有锁定或关闭功能。如：正常运行过程中，应断开维护接口。
10.2.2.3 应具有访问权限控制功能。

10.2.3 失效影响

接口的自身失效不应对安全相关系统执行安全功能产生不期望影响。

10.3 现场设备通信接口要求

10.3.1 安全性要求

10.3.1.1 安全相关系统应能在不影响安全功能的情况下，与非安全相关系统进行通信。

10.3.1.2 安全相关系统的安全通信接口，在逻辑上应独立于与非安全相关系统的通信接口。

10.3.1.3 与安全相关系统连接的设备发生故障时，不应通过通信接口对安全相关系统产生不期望的影响。

10.3.2 安全性验证要求

应对现场设备通信接口和相关软件进行验证，包括：

——失效检测；

——数据确认。

10.4 网络通信接口要求

10.4.1 安全性要求

10.4.1.1 功能安全管理信息系统应利用网络通信接口与安全相关系统进行通信。

10.4.1.2 安全相关系统的网络通信接口和功能安全管理信息系统的网络通信接口应具有逻辑独立性。

10.4.1.3 安全相关系统的设备或功能安全管理信息系统的网络通信接口发生故障，不应影响整个网络正常通信。

10.4.2 安全性验证要求

应对网络通信接口和相关软件进行验证，包括：

——网络区域隔离；

——网络报文的数据完整性。

附 录 A
（资料性）
数字化车间危险与风险分析方法和步骤

A.1 进行危险与风险分析所需的信息

A.1.1 数字化车间的建设内容、设计图纸、平面布置、车间规划。

A.1.2 数字化车间的生产流程、生产工艺等，例如：加工、装配、标定、测试、检验等。

A.1.3 指定的危险与风险分析的范围。

A.1.4 危险与风险分析范围内的数字化车间的各独立功能区域，包括：

——各独立功能区域内的数字化制造设备（如：数字化加工设备、数字化装配设备、数字化物流设备、数字化检测设备、数字化辅助设备等）的功能、动作、操作以及使用限制，以确定正常使用和合理可预见的误用；

——各独立功能区域内的数字化制造设备（如：数字化加工设备、数字化装配设备、数字化物流设备、数字化检测设备、数字化辅助设备等）的管理人员、操作人员、维护人员等相关人员；

——各独立功能区域间的通信接口、通信内容、信息流向以及信息类型；

——各独立功能区域的环境。

A.1.5 当前国内外数字化车间安全相关的法律、法规、标准以及其他相关文件。

A.2 数字化车间危险与风险分析的步骤

A.2.1 制定一套数字化车间危险与风险分析的规程。由数字化车间管理人员、工艺人员、操作人员、维护人员组成的团队负责实施。必要时，可委托第三方实施。

A.2.2 数字化车间危险与风险分析的步骤，见图 A.1。

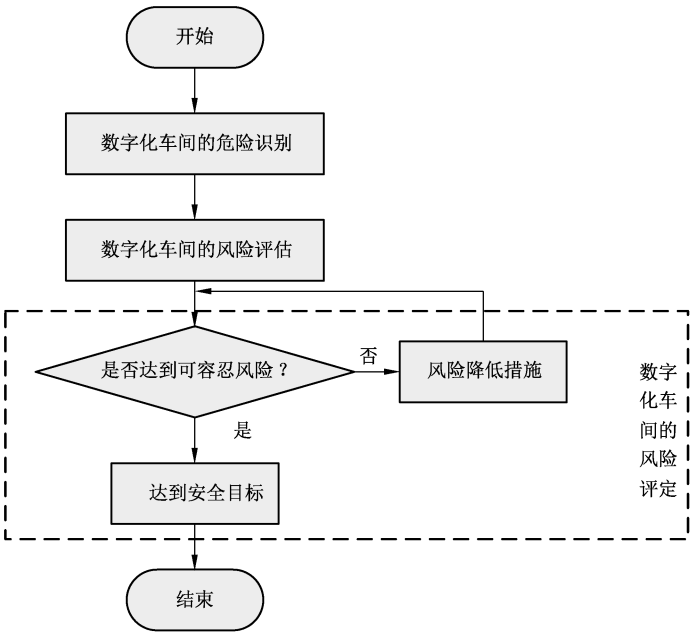

图 A.1 数字化车间危险与风险分析的步骤

A.3 数字化车间的危险识别

A.3.1 在确定的危险与风险分析范围内，进行危险识别。

A.3.2 根据合理可预见的情况（包括：故障状况、合理可预见的误用、恶意或未经授权的行为、所有相关的人为因素引起的问题等），全面识别数字化车间中的危险、危险状态以及危险事件，包括：

——识别与数字化车间的数字化制造设备、数字化辅助设备、信息基础设施、人员直接相关的所有合理可预见的危险、危险状态和危险事件。

——识别与数字化车间的数字化制造设备、数字化辅助设备、信息基础设施、人员不直接相关的所有合理可预见的危险、危险状态和危险事件（例如地震、雷电等）。

——全面识别数字化车间在不同运行模式下，所有合理可预见的危险、危险状态和危险事件。

注 1：数字化车间的不同运行模式包括：调试、运行、维护等。

——如果识别到了合理可预见的、恶意的或未经批准的行动构成了数字化车间的信息安全威胁，则需要开展信息安全风险分析。

注 2：IEC 62443-3-2 标准给出了信息安全风险分析的指南。

注 3：参考 GB/T 41260—2022。

A.3.3 数字化车间中的典型危险，见表 A.1。

表 A.1 数字化车间中的典型危险

序号	危险	危险事件	后果
1	数字化加工设备故障	数字化加工设备失控	人身伤害
			财产损失
			环境污染
			声誉影响
2	数字化装配设备故障	数字化装配设备失控	人身伤害
			财产损失
			环境污染
			声誉影响
3	数字化物流设备故障	数字化物流设备失控	人身伤害
			财产损失
			环境污染
			声誉影响
4	数字化检测设备故障	数字化检测设备失控	人身伤害
			财产损失
			环境污染
			声誉影响
5	数字化辅助设备故障	数字化辅助设备失控	人身伤害
			财产损失
			环境污染
			声誉影响

表 A.1　数字化车间中的典型危险（续）

序号	危险	危险事件	后果
6	数字化制造设备互联集成的故障	数字化制造设备失控	人身伤害
			财产损失
			环境污染
			声誉影响
7	信息基础设施故障	数据信息篡改/泄密 数字化制造设备失控	人身伤害
			财产损失
			环境污染
			声誉影响
8	数字化制造设备与信息基础设施互联集成的故障	数据信息篡改/泄密 数字化制造设备失控	人身伤害
			财产损失
			环境污染
			声誉影响
9	生产过程数据互联集成的故障	数据信息篡改/泄密 数字化制造设备失控	人身伤害
			财产损失
			环境污染
			声誉影响
10	人机交互时的误用	数字化制造设备失控 数据信息篡改/泄密	人身伤害
			财产损失
			环境污染
			声誉影响

注 1：数字化车间中的典型危险包括但不限于上述危险。

注 2：数字化车间生产过程中的各种主要危险，参考 GB/T 13861—2009。

注 3：数字化车间中的各种机械可能出现的危险，参考 GB/T 15706—2012 的附录 B。

注 4：数字化车间中的电气设备可能出现的危险，参考 GB/T 22696.5—2011。

A.3.4　随着科学技术的发展、认知水平的提高以及实践经验的丰富，对数字化车间的危险识别能力、水平需要不断地完善和提高。

A.3.5　危险识别的信息需数字化归档。

A.4　数字化车间的风险评估

A.4.1　对于数字化车间中每个确定的危险事件，需进行风险评估：

a）　评估数字化车间中的每个危险事件所伴随的潜在后果；

b）　评估数字化车间中的每个危险事件的发生率；

c）　根据 a）、b），评估数字化车间中的每个危险事件的风险。可选用定性或定量的方法。

A.4.2　风险评估之后，给出风险评估结果。

A.4.3　风险评估的信息需数字化归档。

A.5 数字化车间的风险评定

A.5.1 对于数字化车间中的每个确定的危险事件，需要根据企业自身的要求，确定其可容忍风险。

A.5.2 可容忍风险与风险评估结果进行比较，确定是否采用风险降低措施。

A.5.3 选择适当的风险降低措施，包括：基于机械、液压、气动、电气/电子/可编程电子等技术的风险降低措施。

A.5.4 实施风险降低措施，最终达到可容忍风险的目标。

附 录 B
（资料性）
安全完整性等级（SIL）与性能等级（PL）之间的关系

B.1 安全完整性等级 SIL

安全完整性等级 SIL 是一种离散的等级（四种可能之一），用于规定分配给 E/E/PE 风险降低措施的安全完整性要求。SIL4 是最高的，SIL1 是最低的。

B.2 性能等级 PL

在 GB/T 16855.1—2018 中，性能等级 PL 为在可预期的条件下，用于规定 SRP/CS 执行风险降低的离散等级。

对于所选的执行安全功能的每个 SRP/CS 和/或 SRP/CS 的组合，都应完成其 PL 的估计。可通过估计以下参数来确定 SRP/CS 的 PL：

——单个元件 $MTTF_D$ 的值；

——DC；

——CCF；

——结构；

——安全功能在故障条件下的表现；

——安全相关软件；

——系统性失效；

——预期环境条件下，执行安全功能的能力。

B.3 PL 和 SIL 之间的关系

PL 和 SIL 之间的关系，见表 B.1。

表 B.1 PL 和 SIL 之间的关系

PL	SIL （运行模式为高/连续）	PFH_D （每小时危险失效平均频率）
a	无对应	$\geqslant 10^{-5} \sim < 10^{-4}$
b	1	$\geqslant 3\times 10^{-6} \sim < 10^{-5}$
c	1	$\geqslant 10^{-6} \sim < 3\times 10^{-6}$
d	2	$\geqslant 10^{-7} \sim < 10^{-6}$
e	3	$\geqslant 10^{-8} \sim < 10^{-7}$

PL＝a 与 SIL 无对应的等级，主要用于轻微的风险减小，通常为可恢复的伤害。SIL4 专门用于流程工业中可能的灾难事件。因此与 SIL3 对应的 PL＝e 级为最高的等级。

参 考 文 献

[1] GB 11291.1—2011 工业环境用机器人 安全要求 第1部分:机器人

[2] GB/T 13861—2009 生产过程危险和有害因素分类与代码

[3] GB/T 15706—2012 机械安全 设计通则 风险评估与风险减小

[4] GB/T 16855.1—2018 机械安全 控制系统安全相关部件 第1部分:设计通则

[5] GB/T 22696.5—2011 电气设备的安全 风险评估和风险降低 第5部分:风险评估和降低风险的方法示例

[6] GB 22998—2008 机床安全 大规格数控车床与车削中心

[7] GB/T 25486—2010 网络化制造技术术语

[8] GB/T 30574—2014 机械安全 安全防护的实施准则

[9] GB/T 32857—2016 保护层分析(LOPA)应用指南

[10] GB/T 41260—2022 数字化车间信息安全要求

[11] IEC 62443-3-2 Security for industrial automation and control systems—Part 3-2: Security risk assessment for system design